UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/584,605	05/31/2000	Peter Bendel	DE9-1999-0058	2850

36736 7590 04/30/2004

DUKE W. YEE
CARSTENS, YEE & CAHOON, L.L.P.
P.O. BOX 802334
DALLAS, TX 75380

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	6

DATE MAILED: 04/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/584,605	BENDEL ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-9,12-14 and 23-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-9,12-14 and 23-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Office Action

Claims 1-5,7-9, and 12-14 are pending. Claims 6, 10, 11, and 15-22 have been canceled. Claims 23-33 have been added and are pending. Claims 1-5,7-9, 12-14, and 23-33 have been considered.

Response to Amendment

The amendment to the specification, on page 5, lines 11-13, is objected to because the resulting sentence is incomplete. Examiner reads the new sentence as "[t]his object is and other means of." The amendment was sent in over a fax and is hard to determine which words are crossed out. Clarification is required.

Response to Arguments

Applicant's arguments filed 3-8-04 have been fully considered but they are not persuasive.

Applicant argues on page 13 with respect to claim 1 that "[n]either the cited portion, nor any other portion of Handel, teaches adding a session ID to a request if a mobile security module successfully authenticates with an authentication module". After

further consideration of the immediate application and the Handel prior art, the examiner respectfully disagrees with applicant.

Claim 1, step dd) states the addition of a session ID to the request if authentication is successful. Neither the claim nor the specification defines what exactly constitutes a session ID. Giving the broadest reasonable interpretation, a session ID is something that uniquely identifies a session from other sessions. Claim 1, as stands does not imply any more description to the term. Therefore, prior art must only teach or reasonably suggest generating a session ID that would distinguish the session from other sessions if authentication is satisfied.

With that interpretation of a session ID one can find uniquely identified sessions in Handel. Handel teaches a user has many personas. Each persona has a unique identifier (column 32, lines 23-26). Handel invention uses this feature to manifest personal information and services based upon which persona a user wants to utilize. As merely an example to the concept, Handel elaborates on a simple example of someone checking into a hotel (column 34, line 59-column 35, line 8). The user must first authenticate by entering a PIN number. It is clearly suggested that if authentication is not satisfied the procedure halts and the connection is stopped. It is also suggested that entering a PIN into a smart card reader is just one embodiment of Handel's teaching. Authentication is met once a server validates the digital certificate. In order to personalize the retrieved information the correct persona must be used and be attached in some way to the subsequent requests. Two things must then occur to present personalized data to the user. The first is that the system must identify which persona

to implement and the second is that the merchant (hotel) must also have the proper credentials to access the information. Handel says that the user gives that permission. It is suggested that the unique identifier could be used to choose the desired persona. The current session ID is then unique in that the session is dependent upon which persona is being used and the merchant. Any combination of persona and merchant would dictate a different session ID. The persona is used to retrieve relevant information while the merchant's identity plays a vital role in what information is displayed to that particular merchant. It is suggested that some merchants could have access to different information.

To summarize, the combination of a persona and merchant creates a session ID to provide particular relevant and obliged information to the two parties. Unique identification is crucial to the invention. As Handel teaches on column 32, lines 22-41, personas can be vastly different and inherit different rights. Therefore in the context of the hotel scenario, a user entering the hotel under a business persona would need to be unique from the same user entering the hotel under a pleasure persona to discriminate between business and pleasure. In view of Handel teachings, the examiner finds that he indeed does disclose and suggest creating a session ID once authentication is complete. One of ordinary skill in the art would then mentally conceive that all subsequent requests during a session would fall under the same session ID until the session is somehow terminated.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 23-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Independent claims 23 and 27 both disclose multiple steps whereby an entity is receiving an object, for example "receiving a session identifier from the server". The language of the claims is indefinite because it is not clear if the client, authentication applet, or neither is receiving the objects. The examiner is interpreting this to mean the authentication applet is receiving the session identifier for examination on the merits. Any similarly, that the client is receiving the authentication applet. However, the examiner bases this interpretation on claim 33 because in that claim, the applet is configured to perform the receiving. This does not infer that the client that is not capable of the receiving. Therefore, the claims should be amended to clearly state which entity is receiving the objects such as the session identifier and the applet.

Claim Rejections - 35 USC ' 102

Claims 1, 2, and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Handel et al (USP 6,195,651).

As per claim 1, Handel et al teach a method and software for controlling access to protected contents on a server, the method requiring the following components to be present:

a) a server (column 34, line 19)

b) a client (column 7, lines 60-66)

c) a reader (chip card reader) for a mobile security module (chip card) (column 34, lines 59-60)

d) a security module (chip card) having at least one protected area for storing a key (column 34, lines 59-60)

e) a data line for communications between client and server characterized by the following steps (column 7, lines 60-66):

aa) sending to the server of a request to call up protected access contents (column 34, line 35)

bb) sending from the server to the client of an authentication module to be run in the client (column 8, lines 35-57)

cc) execution of an authentication protocol for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module (column 7, lines 60-67 and column 34, lines 54-65)

dd) if the authentication in step cc) was successful, addition to the request in step aa) of a session ID which was generated in the course of the communications between

the authentication module and the server (column 34, lines 63-66 and see attached code on column 42, pertaining to Intention List)

ee) sending of the new request to the server application (column 34, lines 63-66)

ff) checking of the session ID in the request to see that it is recorded in the server (column 34, lines 63-66)

gg) processing of the content requested for transmission and searching of the content for further links to other protected-access contents (column 34, line 60—column 35, line 8)

hh) addition of the session ID to the links identified (column 34, line 60—column 35, line 8)

ii) sending of the content modified as in step hh) to the client (column 34, line 60—column 35, line 8).

As per claim 2, Handel et al teach that the server is a web server and the protected contents are web pages which are called up via a browser by a URL request from a client (column 7, lines 60-67).

As per claim 14, Handel et al teach that the session ID generated in step dd) is recorded in a table and in that the presence of an entry in the table is a requirement for access to all the protected-access pages (column 32, lines 23-42).

Claims 23-30, 32-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Laursen et al, hereinafter Laursen (USP 6,065,120).

As per claims 23, 27, and 33 Laursen teaches:

Sending a request for protected content to a server (column 2, lines 48-49);

Receiving an authentication applet (column 14, line 44) and a random number from the server (column 11, lines 63-64);

Executing the authentication applet (column 12, lines 10-15);

Sending the random number to a mobile security module that includes a cryptographic key and generates a cryptographic signature based on the key and random number (column 12, lines 14-15);

Receiving and sending the cryptographic signature from the mobile security module to the server (column 12, lines 45-53);

Receiving a session identifier from the server responsive to the server authenticating the cryptographic signature (column 12, line 60—column 13, line 5).

As per claims 24 and 28, Laursen teaches sending a second request for the protected content to the server wherein the second request includes the session identifier (column 13, lines 3-5).

As per claims 25 and 29, Laursen teaches the mobile security module includes an individual number for the mobile security module and wherein the mobile security

module generates the cryptographic signature based on the individual number (column 10, lines 8-12 and 56).

As per claims 26 and 30, Laursen teaches receiving and sending the individual number from the mobile security module to the server for authentication (column 10, lines 55-60).

As per claim 32, Laursen teaches the client is a Web client (column 14, line 43), wherein the server is a Web server (column 8, lines 10-30), and wherein the protected content is a Web page (column 3, line 15).

Claim Rejections - 35 USC ' 103

Claims 3, 4, 7, 8, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handel et al in view of Hopkins (USP 5,757,918).

As per claim 3, Handel et al teach that the authentication protocol is executed in the followed steps:

mm) sending of the digital signature to the server

nn) checking of the correctness of the digital signature using the security module of the server.

Handel is silent in expressly disclosing that:

jj) generation of a random number by the server application when the content requested is access-protected and the requirements for access have not been satisfied, and sending of the random number to the authentication module

kk) sending of the random number from the authentication module to the mobile security module

ll) generation in the mobile security module of a digital signature which takes account of the identity number of the mobile security module, the random number and the key of the mobile security module

Hopkins teaches:

jj) generation of a random number by the server application when the content requested is access-protected and the requirements for access have not been satisfied, and sending of the random number to the authentication module (column 9, lines 10-15)

kk) sending of the random number from the authentication module to the mobile security module (column 9, lines 15-20)

ll) generation in the mobile security module of a digital signature which takes account of the identity number of the mobile security module, the random number and the key of the mobile security module (column 10, lines 37-42).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Hopkins within the system of Handel et al because the addition of using a random number increases the security of the authentication protocol. Hopkins authentication protocol also helps to insure that

correct owner of a smart card is the one who is using the smart card. Having the random number prevents someone from trying to replay an authentication handshake. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 4, Handel et al teach that the server application is a servlet and the client authentication module is an authentication applet (column 8, lines 35-61). It is inherent that on receipt of a URL request the servlet checks the URL request for the presence of a session ID and if there is no session ID present sends an authentication applet. Handel et al teach that whenever personal data is being accessed that one must first authenticate (column 34, lines 34-66 and column 31, line 45—column 32, line 41). Therefore, a session id or profile must first be authenticated.

Handel et al is silent in disclosing that the request contains a random number to the client. The examiner supplies the same rationale for the motivation as recited in the rejection of claim 3.

As per claims 7 and 8, Handel et al teach that a digital signature is generated with the use of identifying information (column 34, lines 53-66). Handel et al is silent in explicitly disclosing that the digital signature is generated by means of a symmetrical encryption algorithm such as DES or triple DES or by means of an asymmetrical encryption algorithm such as RSA, DSA, or an elliptic curve algorithm. Hopkins teaches digital signature is generated by means of a symmetrical encryption algorithm (DES)

with the help of a secret key agreed between client and server, or by means of an asymmetrical encryption algorithm (RSA) with the help of a private key, the server being in possession of the public key (see column 5, lines 55-60, column 4, line 60—column 5, line 6 and column 7, lines 12-25). The use of symmetrical and asymmetrical digital signatures is well known in the art. One of ordinary skill in the art would be motivated to use either method to encrypt a digital signature as Hopkins teaches.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Hopkins within the system of Handel et al because digital signatures as used by Handel et al are known to be generated in the art by the teachings of Hopkins. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 9, Handel et al teach that error messages are produced whenever errors are generated (column 21, lines 15-22. A failed authentication attempt is an error. Handel et al also teach one must authenticate before access is granted to privileged resources (column 34, lines 33-40). Therefore, it is inherent that Handel et al teach that if the digital signature does not agree, the servlet sends an error message to the client applet.

Claims 5, 12, and 13, are rejected under 35 U.S.C. 103(a) as being unpatentable over Handel et al in view of Lin et al (USP 6,052,785).

As per claim 5, Handel et al teach that the communication between the client and server take place over a secure protocol (column 7, lines 62-63). Handel et al is silent in disclosing that the secure protocol is SSL. Lin et al teaches the use of SSL to securely communicate between a client and server (column 6, line 55—column 7, line 24).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Lin et al within the system of Handel et al because Handel teaches the use of a secure communication protocol and SSL is a secure layer protocol. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claims 12 and 13, Handel et al is silent in disclosing that the session ID, which has a period of validity, loses its validity on expiry of a fixed time or when a session is terminated by means of a log-off page. Lin et al teach that the session ID, which has a period of validity, loses its validity on expiry of a fixed time or when a session is terminated by means of a log-off page (column 6, line 60—column 7, line 24). Handel et al disclose the use of session ID in the form of profiles and personas linked to a user, which has a unique identifier for each of his/her personas, or sessions (column 32, lines 23-42). Each one of the sessions is protected and is of a secure nature.

Therefore, it would have been obvious to one of ordinary skill in the art to protect them with time expirations as taught by Lin et al.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Lin et al within the system of Handel et al because the time expiration helps to prevent a thief from trying to replay an authentication attempt in order to gain access to privileged information. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Claims 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen in view of Handel et al.

As per claim 31, Laursen is silent in discloses the mobile security module is a chip card and includes a chip card reader. The use of such devices increases the security of the system because the private data stored on a chip card is protected. Therefore it would be advantageous for the system of Laursen to include a means of securely storing the private data that the client needs to send to the server for authentication. Handel et al teach the use of a chip card and reader for this purpose (column 34, lines 59-60). In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Handel et al within the system of Laursen because it would allow the user of the client to securely store the private authentication data.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100